**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

What is claimed is:

1. (Currently Amended) A method of processing a message to determine a tag value from the message and from a key according to a message authentication code, the method comprising:

selecting one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, wherein the data item is derived from the message consists of said message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; [[and]]

determining the tag value to be the selected symbol[[.]];

determining said data item to be a hash value of a one-way hash function calculated from the message;

communicating at least a contribution to the message from a sender to a receiver via a first communications channel; and

communicating the tag value and/or the key from the sender to the receiver via a second communications channel different from the first communications channel.

2. - 3. (Canceled)

4. (Original) A method according to claim 1, wherein the key is short enough to be communicated via a user interaction.

5. (Original) A method according to claim 1, wherein the error correcting code is a Reed-Solomon code and wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key.

6. (Original) A method according to claim 1, wherein the tag value is an element in a finite field.

7. (Canceled)

8. (Original) A method according to claim 7, wherein the second communications channel includes a user interaction.

9. (Currently Amended) A communications device for communicating data messages, the communications device comprising:

a transmitting/receiving circuitry operable on a first communication channel operable to transceive at least a contribution to a message via the first communications channel;

a transmitting/receiving circuitry operable on a second communication channel operable to transceive a tag value and a key via the second communications channel;

~~processing means that is adapted~~ a processor operable to determine [[a]] the tag value from [[a]] the message and from [[a]] the key according to a message authentication code, and wherein the ~~processing means~~ processor is further ~~adapted~~ operable to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected, and wherein the processing means is further adapted to determine the tag value to be the selected symbol.

10. (Currently Amended) A computer program product embodied on a computer readable medium loaded into a memory and executed by a processor comprising:

instructions to control a transmitting/receiving circuitry operable on a first communication channel to transceive at least a contribution to a message via the first communications channel and a transmitting/receiving circuitry operable on a second communication channel operable to transceive a tag value and a key via the second communications channel;

instructions causing the processor to determine a tag value from a message and from a key according to a message authentication code, further comprising:

instructions causing the processor to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

instructions causing the processor to determine the tag value to be the selected symbol.

11. (Currently Amended) A computer program product embodied on a computer readable medium loaded into a memory and executed by a processor comprising:

instructions to cause the processor to communicate data messages over a first communications channel;

instructions to cause the processor to determine a tag value from a message and from a key according to a message authentication code sent over a second communications channel;

instructions to cause the processor to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

instructions to cause the processor to determine the tag value to be the selected symbol.

12. (Currently Amended) A communications device for communicating data messages, the communications device comprising:

a receiving circuitry operable on a first communication channel operable to receive at least a contribution to a message via the first communications channel;

a receiving circuitry operable on a second communication channel operable to receive a tag value and a key via the second communications channel;

a processing unit ~~that is adapted~~ operable to determine [[a]] the tag value from a message and from [[a]] the key according to a message authentication code, and wherein the processing unit is adapted to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected, and wherein the processing unit is adapted to determine the tag value to be the selected symbol.